Cellebrite

PHYSICAL ANALYZER

Physical Analyzer, Logical Analyzer, Cellebrite Reader, and UFED Cloud

Release Notes

June 2023 | Version 7.62.2

Cellebrite

Here's What's New in Cellebrite Physical Analyzer Version 7.62.2

363	12,642	69
Total Apps Supported	**Total Versions Supported**	**Updated Parsers**

Important Notice – Hotfix

Physical Analyzer version 7.62.2 includes a hotfix for the issue described below.

- We identified an issue with the License Loader that could lead to a failure. If the upgrade to version 7.62.1 was successful, there is no need to install version 7.62.2.
- An issue was identified with Facebook where information within certain records may cause PA to crash. The PA7.62 Hotfix introduced validation checks to ensure that problematic records are managed appropriately, and a crash does not occur.

  The issue stemmed from the fact that Physical Analyzer parses both Posts and Comments from Facebook and is able to recognize the important parent/child relationship between the two items.

  However, in some cases, posts included information that identifies itself as its own parent. This cyclical relationship caused PA to crash as it struggled to create an infinite relationship between an object and itself.

Updated Decoding Capabilities

Android

- Signal Private Messenger Backup
  Physical Analyzer now supports the latest Signal backup extractions for Android (Version 6.22)
- MEGA Chat
  Mega is a Cloud storage platform that has been on the market since 2005.
  Physical Analyzer can now support the chat component of the MEGA application for Android. This includes support for chats, contacts, messages, locations, and calls.

- WhatsApp Unread Message Indication
  Physical Analyzer returns the "unread" message icon for incoming unread WhatsApp Messages.

- WeChat
  Physical Analyzer now includes multiple improvements for WeChat, including:
  - Improved contact parsing
  - Improved attachment parsing
  - Bug fixes for system message sender and device owner for messages
  - Added a label containing the name of the shared location to location-sharing messages. Improved call message parsing.

- Yahoo Mail

  Physical Analyzer now supports the latest version of Yahoo Mail for Android, including Mails, Contacts, and User Accounts.

- **IMO HD**

  Physical Analyzer now supports the latest support for IMO HD Android (version 2023.02.3038)

  Added parsing capabilities of additional artifacts: Contacts, Locations, Calls, Chat, Text Messages and Attachments (emoji, Sticker, files, URL, images, videos, voice message), System messages, and User account.

- Google Takeout – Google Chats

  Physical Analyzer now supports Google Takeout chat (previously Hangouts) for the following data types:

  - Chat/Messages
  - Contact
  - Calendar entries

iOS

- More Biome Support

  Physical Analyzer has expanded the number of artifacts supported by iOS Biome. PA can now parse the screen On/Off state 'Backlight'.

- WeChat

  Physical Analyzer now includes multiple improvements for WeChat, including:

  - Improved contacts parsing
  - Added a label containing the name of the shared location to location-sharing messages.
  - Improve call message parsing.

- Support for the latest version of IMO iOS

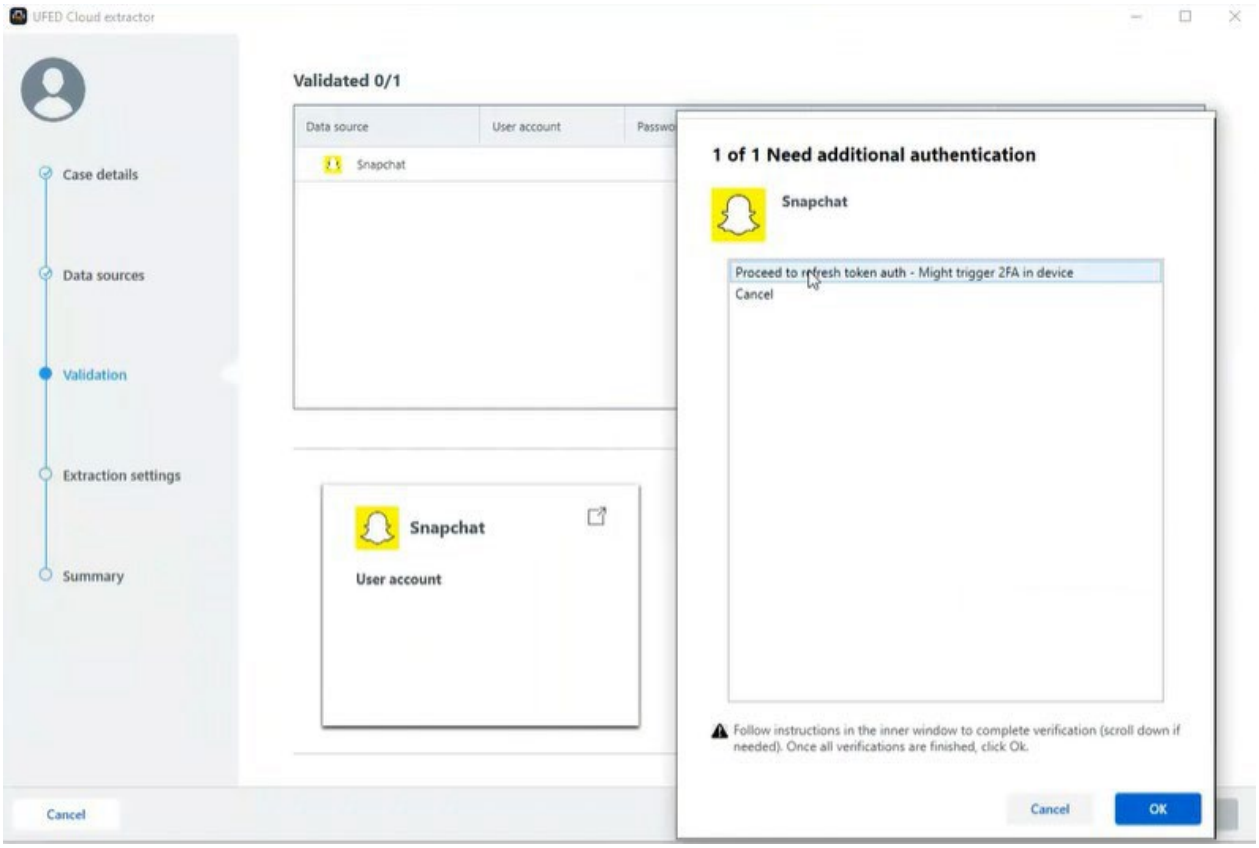
This version provides updated support for the IMO application. (Version 2023.02.0202)

Added parsing capabilities of additional artifacts: Contacts, Locations, Calls, Chat: Text Messages and Attachments (emoji, Sticker, files, URL, images, videos, voice message), System messages, and User account.

Cloud

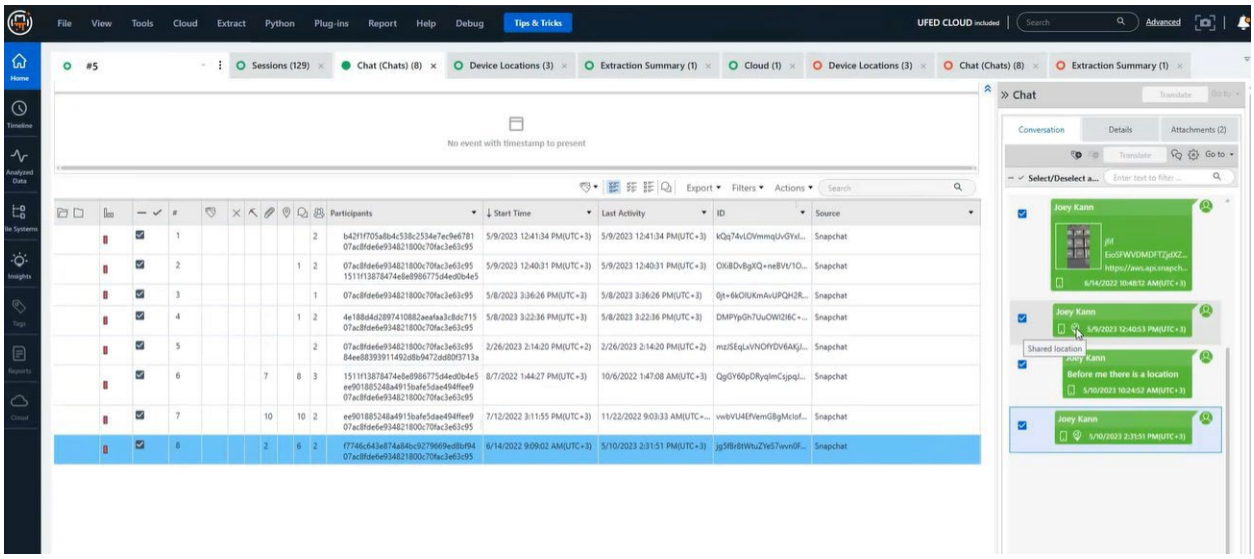
Snapchat offline account enablement

- Due to changes made by Snapchat to the user authentication process, support for extracting secondary (offline) accounts via Account Package, that was temporarily disabled, is now enabled.
- A warning popup will be displayed to enable the usage of refresh token authentication, potentially triggering 2FA. This popup is a prerequisite for refresh token authentication. The authentication process proceeds only upon user approval and may prompt 2FA on the device.



Snapchat shared location information.

UFED Cloud now supports shared location from Snapchat.


File
View
Tools
Cloud
Extract
Python
Plug-ins
Report
Help
Debug
Tips & Tricks
UFED CLOUD included
Search
Advanced
#5
Sessions (129)
Chat (Chats) (8)
Device Locations (3)
Extraction Summary (1)
Cloud (1)
Device Locations (3)
Chat (Chats) (8)
Extraction Summary (1)
No event with timestamp to present
Export
Filters
Actions
Search
Participants
Start Time
Last Activity
ID
Source
Snapchat
Chat
Translate
Conversation
Details
Attachments (2)
Go to
Select/Deselect a...
Enter text to filter ...
Joey Kann
6/14/2022 10:48:52 AM(UTC+3)
Joey Kann
5/9/2023 12:40:53 PM(UTC+3)
Shared location
Joey Kann
Before me there is a location
5/10/2023 10:24:52 AM(UTC+3)
Joey Kann
5/10/2023 2:31:51 PM(UTC+3)

Solved Issues

- Kik Messenger (iOS)
  An issue was identified where an icon may be displayed as a Kik Message attachment instead of the intended media item. The issue was related to both files being present within a single binary plist.
- Discord Warrant Return not parsing
  An issue was identified due to a change made to the Warrant Return data provided by Discord. These changes are now handled within PA.
- WeChat attachments are not opening.
- Google Takeout Parser is not parsing chats (Hangouts)
  This was not supported, since changing to chats and was resolved by the addition of the Google Chats parser.
- Facebook Warrant Returns
  Solved an issue caused by a change to Facebook Warrant Return data where PDF files were used to provide information.
- GrayKey iOS Extractions

  Solved an issue with some Graykey iOS Extractions where processing would run indefinitely.
- PA Unable to parse large Facebook takeouts.
- iOS GrayKey | Analyzed Data - Instagram Searched Items - "Cellebrite.Decoding.Evidence.com"
- iPhone 13 - IOS 16.2 GrayKey Not parsing the WhatsApp.
- PA 7.61 iOS 16.3 iPhone 13 Wrong Sim indication
- WeChat Android - Parse modified identifier for contacts.
- CashApp data not displaying correctly (iOS)
  An issue was resolved where in some circumstances, the sender and recipient of transactions were displayed in the opposite way. (The sender was displayed as the recipient and the recipient was displayed as the sender.)
- PA 7.60 Deleted Date timestamp is incorrect.
- PA 7.58 Facebook warrant return PDF version
- PA 7.57 Apple iCloud warrant return native messages different between versions.
- iCloud Warrant Returns - multiple accounts bugs.
- PA CS | 8.4 | Snapchat iOS | Wrong User account name if the username change

New and updated apps

Android

# Updated Apps - Android	
Bit Pay	14.7.8
Chrome	110.0.5481.65
Coinbase	28.16.0
Facebook	405.0.0.23.72
Facebook Messenger	407.0.0.11.104
Firefox	110.0.1
Gmail	2022.10.30.488439685.Release
Google Drive	2.22.457.2.all.alldpi
Google Maps	11.66.0602
Google photos	6.15.0.490613891
Instagram	271.1.0.21.84
KakaoTalk	9.9.7
Kik Messenger	15.49.0.27501
Line	12.20.2
Metamask	5.11.0
My Ether Wallet	2.5.1
Session	6.11.7
Signal Private Messenger	6.11.7
Skype	8.94.0.426
SnapChat	12.32.0.35
Telegram	9.6.4
TikTok	28.3.4
Trust Wallet	6.57.1
Twitter	9.76.0-release.0
Viber	19.4.0.0
WeChat	8.0.34
WhatsApp Business	2.22.23.84
Wickr	6.2.7

WhatsApp	2.23.10.2
Keepsafe	11.4.0
Web.de	7.10.4
GMX	7.11.1
KakaoMaps	5.7.0
KakaoTaxi	5.21.0
Imo	2023.04.1071
Yahoo Mail	7.14.2
MEGA	8.0

iOS

Chrome	110.5563.101
Coinbase	28.17
Facebook	405.1
Facebook Messenger	406.0.0.30.114
Firefox	111.1
Gmail	6.0.221113
Google Maps	6.55.0
Instagram	270
KakaoTalk	9.9.8
Kik Messenger	16.8.1
Line	13.1.0
Metamask	5.11.0
My Ether Wallet	1.8.2
Privet Photo Vault	14.8
ProtonMail	4.1.1
Signal Private Messenger	6.12.0
Skype	8.94.3422
SnapChat	12.31.0
Telegram	9.6.2
TikTok	28.2.0

Trust Wallet	7.22
Twitter	9.45
Viber	19.4.1
WeChat	8.0.32
WhatsApp Business	22.23.77
Wickr	6.4.2
Session	2.2.7
Web.de	8.43
GMX	8.37
WhatsApp	2.23.8.78
imo	2023.02.0202

Cellebrite
PHYSICAL
ANALYZER

The Industry Standard for Digital Data Examination

Read more about Physical Analyzer here

Update your Physical Analyzer today

Cellebrite